



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,482	04/09/2004	Barry Steven Herman	L111US	1214
30368	7590	11/30/2007		
EMC CORPORATION 6801 KOLL CENTER PARKWAY PLEASANTON, CA 94566			EXAMINER LOUIE, OSCAR A	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 11/30/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mw

<b>Office Action Summary</b>	<b>Application No.</b> 10/821,482	<b>Applicant(s)</b> HERMAN, BARRY STEVEN	
	<b>Examiner</b> Oscar A. Louie	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 04 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1 and 3-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, and 3-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

This final action is in response to the amendment filed on 10/04/2007. The examiner acknowledges the amendments to Claims 1, 3, 4, 9, & 16 and the cancellation of Claim 2, as well as, the amendments to the specification. In light of the amendments, the examiner hereby withdraws his objections in regards to the specification and 35 U.S.C. 2<sup>nd</sup> paragraph rejection in regards to Claim 1. Claims 1 & 3-20 are pending and have been considered as follows.

### *Claim Rejections - 35 USC § 103*

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1 & 3-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Raith (US-5241598-A) in view of O'Connell (US-5991882-A).

Claim 1:

Raith discloses a method of resetting a key for accessing a computer program, but does not explicitly disclose,

- "setting a flag to indicate that the key is to be reset," although Raith does suggest the usage of flags for a key reset, as recited below;

- “starting a process associated with the program,” although Raith does suggest the execution of an algorithm in a network, as recited below;
- “determining, when the process has been started, whether the flag is set,” although Raith does suggest the resetting of a flag under specific conditions, as recited below;
- “resetting the key to a default value based on the flag,” although Raith does suggest resetting a key to a selected value which may be a default value, as recited below;

and does not at all disclose,

- “wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value,” although O’Connell does disclose several figures involving password resetting, as recited below;

however, Raith does disclose,

- “including in a message sent from the network to the mobile station an order or a signal (flag) to reset the B-key” [column 30 lines 52-53];
- “Execution of the authentication algorithm in the home network” [column 17 lines 37-38];
- “The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message” [column 30 lines 65-68 & column 31 lines 1-3];

- “According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value” [column 30 lines 38-42];

where as O'Connell does disclose,

- [Fig 3 & 4 illustrate the resetting of a password (i.e. key) by a user with a proper level of authorization (i.e. prescribed level of privilege) without the intervention of an administrator (i.e. without intervention of a provider)];

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, “setting a flag to indicate that the key is to be reset” and “starting a process associated with the program” and “determining, when the process has been started, whether the flag is set” and “resetting the key to a default value based on the flag” and “wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value,” in the invention as disclosed by Raith for the purposes of automated password (i.e. key) resetting.

Claim 3:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 1 above, their combination further comprising,

- “logging in with, sufficient privileges to start the process” (i.e. “To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network”) [column 32 lines 4-7].

Claim 4:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 1 above, their combination further comprising,

- “the flag is an environment variable” (i.e. “The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station”) [column 30 lines 61-64].

Claim 5:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 4 above, their combination further comprising,

- “resetting the key to a default value includes instructing a database system to reset the key” (i.e. “According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value” [column 30 lines 38-42].

Claim 6:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 4 above, their combination further comprising,

- “unsetting the flag” (i.e. “The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station”) [column 30 lines 61-64].

Claim 7:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 6 above, their combination further comprising,

- “starting the process again” (i.e. “When the mobile subscriber crosses over into another area, the exchange associated with that area, upon receiving an identity signal from the telephone unit, will record an indication of the mobile subscriber's presence there and then transmit the identity signal to all of the other exchanges together with its own identity signal, for the purpose of updating the mobile subscriber's position”) [column 2 lines 59-66].

Claim 8:

Raith and O'Connell disclose a method of resetting a key for accessing a computer program, as in Claim 6 above, their combination further comprising,

- “changing the key from the default value to a secure value” (i.e. “Where encryption is desired, a new S-key must be calculated since the previous S-key was calculated using the previous B-key which was out of synchronization”) [column 31 lines 10-13].

Claim 9:

Raith discloses a system for resetting a key for accessing a computer program, comprising a computer, but does not explicitly disclose,

- “determine whether a flag is set, when a process associated with the computer program is started,” although Raith does suggest the resetting of a flag under specific conditions, as recited below;

- “reset the key to a default value, based on the flag,” although Raith does suggest resetting a key to a selected value which may be a default value, as recited below;

and does not at all disclose,

- “wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value,” although O'Connell does disclose several figures involving password resetting, as recited below;

however, Raith does disclose,

- “The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message” [column 30 lines 65-68 & column 31 lines 1-3];
- “According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value” [column 30 lines 38-42];

where as O'Connell does disclose,

- [Fig 3 & 4 illustrate the resetting of a password (i.e. key) by a user with a proper level of authorization (i.e. prescribed level of privilege) without the intervention of an administrator (i.e. without intervention of a provider)];



Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, "determine whether a flag is set, when a process associated with the computer program is started" and "reset the key to a default value, based on the flag" and "wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value," in the invention as disclosed by Raith for the purposes of automated password (i.e. key) resetting.

Claim 10:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 9 above, their combination further comprising,

- "configured to require administrator privileges to start the process" (i.e. "To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network") [column 32 lines 4-7].

Claim 11:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 10 above, their combination further comprising,

- "the flag is an environment variable" (i.e. "The B-key reset flag may consist of any number of bits and, in the simplest case, may be no more than a single bit (1 or 0) assigned to a specific field in the message transmitted from the network to the mobile station") [column 30 lines 61-64].

Claim 12:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 11 above, their combination further comprising,

- “a database system configured to store the key” (i.e. “the HLR has no voice transmission, reception or switching facilities, but is essentially a database from and to which information can be read and written”) [column 15 lines 7-9];
- “the system is configured to reset the key by instructing the database system to reset the key” (i.e. “the network can retrieve information pertaining to that particular mobile station, e.g., security keys, from the location or database”) [column 15 line 68 & column 16 lines 1-2].

Claim 13:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 9 above, their combination further comprising,

- “the key is associated with an administrator account for accessing the computer program” (i.e. “To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network”) [column 32 lines 4-7].

Claim 14:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 9 above, their combination further comprising,

- “the computer program executes on the computer” (i.e. “an authentication algorithm executed in each of the mobile station and the network”) [column 7 lines 62-64].

Claim 15:

Raith and O'Connell disclose a system for resetting a key for accessing a computer program, comprising a computer, as in Claim 9 above, their combination further comprising,

- “the computer program executes on a second computer” (i.e. “an authentication algorithm executed in each of the mobile station and the network”) [column 7 lines 62-64].

Claim 16:

Raith discloses a computer program product for resetting a key for accessing a computer program, comprising a computer usable medium having machine readable code embodied therein, but does not explicitly disclose,

- “determining whether a flag is set, when a process associated with the computer program is started” although Raith does suggest the execution of an algorithm in a network, as recited below;
- “resetting the key to a default value, based on the flag,” although Raith does suggest resetting a key to a selected value which may be a default value, as recited below;

and does not at all disclose,

- “wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value,” although O'Connell does disclose several figures involving password resetting, as recited below;

however, Raith does disclose,

- “The network may reset the B-key value in the network to the selected value immediately before or at the time of activating the B-key step flag, i.e., setting the bit-value equal to 1 for example, in an order message sent to the mobile station or immediately after receiving from the mobile station an acknowledgement of the order message” [column 30 lines 65-68 & column 31 lines 1-3];
- “According to the present invention, resynchronization of the B-key used by the network and the mobile station may be accomplished by resetting the B-key input to AUTH in each of the network and the mobile station to a selected value” [column 30 lines 38-42];

where as O'Connell does disclose,

- [Fig 3 & 4 illustrate the resetting of a password (i.e. key) by a user with a proper level of authorization (i.e. prescribed level of privilege) without the intervention of an administrator (i.e. without intervention of a provider)];

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, “determining whether a flag is set, when a process associated with the computer program is started” and “resetting the key to a default value, based on the flag” “wherein a prescribed level of privilege is required to start the process such that a user having the prescribed level of privilege but not the key can without intervention of a provider with which the computer program is associated cause the key to be reset to the default value,” in the invention as disclosed by Raith for the purposes of automated password (i.e. key) resetting.

Claim 17:

Raith and O'Connell disclose a computer program product for resetting a key for accessing a computer program, comprising a computer usable medium having machine readable code embodied therein, as in Claim 16 above, their combination further comprising,

- “a database system configured to store the key” (i.e. “the HLR has no voice transmission, reception or switching facilities, but is essentially a database from and to which information can be read and written”) [column 15 lines 7-9];
- “resetting the key includes instructing the database system to reset the key” (i.e. “the network can retrieve information pertaining to that particular mobile station, e.g., security keys, from the location or database”) [column 15 line 68 & column 16 lines 1-2].

Claim 18:

Raith and O'Connell disclose a computer program product for resetting a key for accessing a computer program, comprising a computer usable medium having machine readable code embodied therein, as in Claim 16 above, their combination further comprising,

- “the key is associated with an administrator account for accessing the computer program” (i.e. “To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network”) [column 32 lines 4-7].

Claim 19:

Raith and O'Connell disclose a computer program product for resetting a key for accessing a computer program, comprising a computer usable medium having machine readable code embodied therein, as in Claim 16 above, their combination further comprising,

- “code for requiring sufficient privileges to start the process” (i.e. “To guard against this risk, the performance of a B-key reset may be linked to the performance of bilateral authentication, i.e., to the validation of the network”) [column 32 lines 4-7].

Claim 20:

Raith and O'Connell disclose a computer program product for resetting a key for accessing a computer program, comprising a computer usable medium having machine readable code embodied therein, as in Claim 16 above, their combination further comprising,

- “code for changing the key from the default value to a secure value” (i.e. “Where encryption is desired, a new S-key must be calculated since the previous S-key was calculated using the previous B-key which was out of synchronization”) [column 31 lines 10-13].

***Conclusion***

3. Applicant's arguments with respect to independent Claims 1, 9, & 16 and their dependents have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendment(s).

Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.


Application/Control Number:  
10/821,482  
Art Unit: 2136

Page 15

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL  
11/27/2007

Nasser Moazzami  
Supervisory Patent Examiner

  
11/28/07